Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2016 covering the prior calendar year 2015

1. Date Filed: February 24, 2016

2. Name of Company covered by this certification: Nexus Systems, Inc.

3. Form 499 Filer ID: 823810

4. Name of signatory: Mark Stevenson

5. Title of signatory: President

I, Mark Stevenson, certify that I am an officer of Nexus Systems, Inc. and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures, as summarized in the attached statement, that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI. The company does not have any material information with respect to the process pretexters are using to attempt to access CPNI. Nor has the company taken actions (*i.e.,* proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17, which requires truthful and accurate statements to the Commission and acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Mark Stevenson, President

Nexus Systems, Inc.

STATEMENT EXPLAINING HOW THE COMPANY'S OPERATING PROCEDURES ENSURE COMPLIANCE WITH THE FCC'S CPNI RULES

The following demonstrates Nexus Systems, Inc. ("Nexus," "Company") understanding of and obligation to protect Customer Proprietary Network Information ("CPNI") and describes the Company's policies and business practices intended to protect the confidentiality of CPNI. Nexus has designed these polices and practices to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq*. CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

I. §64.2005 Use of customer proprietary network information without customer approval.

Pursuant to the requirements of 47 C.F.R. § 64, Nexus is allowed to and may use, disclosure, or permit access to CPNI without customer approval to provide or market service offerings among the categories of service to which the customer already subscribes from the Company, including, but not limited to, local and interexchange service.

Nexus provides different categories of service. In the event that a customer subscribes to more than one of the categories of service offered by the Company, Nexus is authorized to and may share CPNI among the Company's affiliated entities that also provide a service offering to the customer. If a customer does not subscribe to more than one of the Company's service offerings, Nexus is not permitted to and does not share CPNI with its affiliates, except as allowed in 47 C.F.R. § 64.2007(b).

Except as provided in 47 C.F.R. § 64.2005(c), Nexus is not allowed to and does not use, disclose, or permit access to CPNI to market to a customer a category of service that that the subscriber does not already subscribe to, without first obtaining approval to do so.

As a wireline carrier, Nexus is authorized to and may use, disclose or permit access to CPNI that results from its provision of local exchange or interexchange service for the delivery of the equipment and services specified in 47 C.F.R. § 64.2005(b)(1) and may do so without customer approval.

Nexus does not use, disclose or permit access to CPNI to identify or track customers who call competing service providers.

Nexus is authorized to and may use, disclose or permit access to CPNI, without customer approval, for the delivery of inside wiring installation, maintenance, and repair services.

As a local exchange carrier (LEC) and an interconnected VoIP service provider, as that term is defined in 47 C.F.R. § 9.3, Nexus is permitted to and may use CPNI to market services such as, but not necessarily limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and particular centrex features and may do so without customer approval.

Nexus is also authorized to and may use, disclose, or permit access to CPNI to protect the rights or property of the Company or to protect users of its or another company's services from fraudulent, abusive, or unlawful use of, or subscription to, such services and is authorized to do so without customer approval.

II. §64.2007 Approval required for use of customer proprietary network information.

In instances where customer approval to use, disclose or permit access to CPNI is required, Nexus will obtain such approval through written, oral, or electronic methods. The Company understands that oral approval must demonstrate compliance with the Commission's Rules.

Approval or disapproval obtained by the Company will remain in effect until the customer revokes or limits such approval or disapproval.

Records of all approvals will be maintained for a period of not less than one year.

Use of Opt-Out and Opt-In Approval Process

Subject to opt-out or opt-in approval, Nexus is allowed to and may use its customer's individually identifiable CPNI for the purpose of marketing communications-related services. The Company is also allowed to and may disclose a customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services and is also allowed to and may permit such persons or entities to obtain access to such CPNI for such purposes.

Except as permitted under 47 C.F.R. § 64.2005, § 64.2007, or section 222 of the Communications Act, Nexus may only use, disclose, or permit access to its customer's individually identifiable CPNI if it has obtained such approval through the use of opt-in approval.

III. §64.2008 Notice required for use of customer proprietary network information.

Notification, Generally

Before soliciting a customer for approval, Nexus will provide notification to the customer of his or her right to restrict the use and disclosure of and access to CPNI as follows:

The Company will retain all record of notification for a period of not less than one year.

Notices to use, disclose, or permit access to a customers' CPNI, will be provided to customers on an individual basis.

Content of Notice

Information in the notification will be sufficient to enable the customer to make an informed decision as to whether to allow use or disclosure, or to permit access to the customer's CPNI and will state the customer's right, and the Company's duty, under federal law, to protect the confidentiality of CPNI. Notifications will specify the type of information that makes up CPNI. the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and are required to inform the customer of his/her right to disapprove those uses and deny or withdraw access to CPNI at any time.

Notifications will advise the customer of what they must do in order to grant or deny access to CPNI, and will inform the customer that denial of approval will in no way affect the provision of any service to which the customer subscribes. Not withstanding the preceding, the Company may include a statement describing any consequences that could result from the lack of access to CPNI.

Notifications will be clear, neutral and legible, will be comprehensible, will not be misleading, will use large enough type to be easily read, and will be placed so as to be apparent to the customer.

Nexus will not translate a part of a notice into a language other than English, but will instead provide a notification that translates all portions into that language.

The Company may include language stating that approval of CPNI may enhance its ability to offer customized products and services and may also state that the customer, upon affirmative written request, can require the Company to disclose CPNI to any person.

Nexus will not use language that encourages the customer to freeze third party access to CPNI.

Notifications will state that approval or denial of the use of CPNI for a service, other than the service the customer already subscribes to, will remain valid until the customer affirmatively revokes or limits the approval or denial. CPNI rights notification and solicitation for approval are to be located adjacent to each other.

Notice Requirements Specific to Opt-Out

In situations where Nexus uses notification to obtain opt-out approval the Company will do so as follows:

Notifications will use electronic or written methods that meet the requirements of 47 C.F.R. § 64.2008(c). Except as provided in 47 C.F.R. § 64.2008(f), oral communications are not allowed.

After providing a notice and opportunity for an opt-out approval, Nexus will wait at least 30 days before assuming approval to use, disclose, or permit access to CPNI. Notifications will inform the customer of the applicable waiting period. The waiting period for electronic notification begins with the date on which the notification was sent while the waiting period for notifications by mail begin on the third day following the date the notification was mailed.

Nexus will provide new notification and opportunity for opt-out approval every two years.

In the event that Nexus sends notices via email, it will first acquire the customer's permission to do so. CPNI opt-out notices, sent via email, must be directly replied to by the customer. Email notices returned as "undeliverable" must be sent to the customer in another form before the notice will be considered received. The subject line of emailed CPNI notices are required to accurately identify the subject matter of the email and Opt-out methods must be provided at no cost to the customer and must be made available 24 hours a day, seven days a week.

Notice Requirements Specific to Opt-In
In situations where Nexus uses notification to obtain opt-in approval the Company will do so as follows:

The Company may obtain opt-in approval through oral, written, or electronic means. Notifications will comply with the requirements of 47 C.F.R. § 64.2008(c).

Notice Requirements Specific to One-Time Use of CPNI
In situations where Nexus uses notifications to obtain one-time use of CPNI, it will do so as follows:

Nexus may use oral notice to obtain limited, one-time use of CPNI for both inbound and outbound for customer contacts via telephone only for the duration of a call placed to obtain opt-out or opt-in approval.

Contents of such notification must comply with the requirements of 47 C.F.R. § 64.2008(c). Notifications that are not relevant to the limited use for which the Company seeks CPNI may omit the following:

No action is required to maintain the opt-out election that has been previously received and no the Company is not required to inform a customer if they have previously opted-out;

The Company is not required to advise customers that CPNI may be shared with affiliates or third parties, or name the same, if the limited use of CPNI will not result in use or disclosure to the affiliate or third party;

Nexus is not required to disclose the a customer can use to deny or withdraw future access to CPNI as long as the Company explains that the scope of approval being sought is limited to one-time use; and

Nexus is not required to tell the customer of the steps that must be taken to grant or deny access to CPNI as long as the Company informs the customer that access to CPNI can be denied for the call.

IV. §64.2009 Safeguards required for use of customer proprietary network information.

Nexus has implemented a system that establishes the status of a customer's CPNI approval prior to the use of CPNI by the Company.

The Company maintains a record of the sales and marketing campaigns of it and its affiliates' that uses a customers' CPNI and maintains a record of all instances where CPNI has been disclosed and/or provided to a third party, or where a third party has been allowed access to a customers' CPNI. All records include a description of the campaign, the specific CPNI used, and the products and services that were offered. All records are maintained for no less than a one-year period of time.

Nexus trains its personnel as to the rules for customer authorization of CPNI, which includes when the Company is and is not authorized to use CPNI. Nexus has also implemented a disciplinary policy for violation of the Company's CPNI policy. A supervisory review process has also been established for compliance with the requirements of the FCCs CPNI Rules and a record of the Company's compliance of the same is maintained for a period of not less than one year. Company personnel are required to obtain a supervisor's approval of any outbound marketing request for customer approval of CPNI.

On an annual basis, Nexus files a compliance certification signed by an officer of the Company, which states that the officer has personnel knowledge that the Company has established operating procedures that are adequate to ensure compliance with the FCC's CPNI Rules. In addition, the Company provides an accompanying statement explaining how the Company's operating procedures are in compliance with the Commission's CPNI Rules, explains any actions taken against data brokers, and provides a summary of all customer complaints received in the previous year concerning unauthorized release of CPNI.

The Company will notify the Commission of any instance in which the Company's opt-out mechanism does not allow customer's to opt-out as specified by the Commission's Rules and will do so within five (5) business days of discovery of the same. The notice to the Commission will be provided in the form of a letter and will include a description of the Company's opt-out mechanism, the problem, the proposed remedy and when the remedy was or will be implemented. The notice will also state whether the relevant state commission has been notified and any action taken by the same. A copy of the notice sent to customers will also be provided.

V. §64.2010 Safeguards on the disclosure of customer proprietary network information.

Nexus has measures in place designed to discover and protect against unauthorized access to CPNI, which includes authentication of a customer before disclosing CPNI when requested during a customer-initiated telephone call or online account access.

Telephone access to CPNI

In the event of a request made during a customer-initiated telephone call, customers are first required to establish and use a password before Nexus will provide call detail information to the customer by phone. Once established, the customer is required to provide the password without

help from or prompting by Company personnel. Company personnel are not allowed to perform customer authentication based on biographical or account information.

If the customer has not established or is unable to provide the password, the Company will provide call detail information to the customer by sending to the customer's address of record.

Online access to CPNI

As is the case with telephone access to CPNI, customer authentication is required for online access to CPNI, which is provided through the use of a customer-established password. Customer is required to provide the password without help from or prompting by Company personnel. Company personnel are not allowed to perform customer authentication based on biographical or account information. Once authentication has been successfully completed, the customer will be allowed to obtain access to CPNI that is directly related to a telecommunications service account.

Password establishment and Back-up Authentication Methods for Lost or Forgotten Passwords

Nexus has developed a procedure whereby a customer can create an authentication password that does not rely or depend on customer biographical or account information. The Company has also created a procedure to allow back-up authentication that can be used in the event that a customer has lost or forgotten his/her password. A customer that is unable to provide their authentication password is required to establish a new password.

Notification of account changes

Nexus immediately notifies a customer in the event of a creation of or change to a password or a customer response to a back-up authentication for lost or forgotten passwords, online account, or address of record creation or change. Notification is provided using a company provided voicemail, text message to the telephone number of record, or by mail to the address of record. Notifications do not include the changed information.

Businesses may instead contractually bind themselves to authentication methods other than those described above.

VI. §64.2011 Notification of customer proprietary network information security breaches.

Nexus will notify law enforcement of a breach of customer CPNI. Notification will be handled consistent with state or local laws. Within seven (7) business days after determination that a breach has occurred, the Company will notify the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI"). Nexus will not notify customers or publicly disclosure the breach until seven (7) days after notification to the USSS and the FBI unless otherwise allowed to do so by the relevant investigating agency.

Neither customer notification nor public disclosure will occur until the Company has completed the required notification of law enforcement. Should the Company believe notification sooner than allowed, it will do so only after consulting with the relevant investigating agency. Customer notification will commence upon completion of the process of notifying law enforcement.

Nexus will retain a record of any breaches discovered, notifications made to law enforcement, USSS and the FBI, and notifications to its customers for a period of not less than two (2) years. If available, records will include the date of discovery, notification, and detail and circumstances of the breach.

Dated February 24, 2016